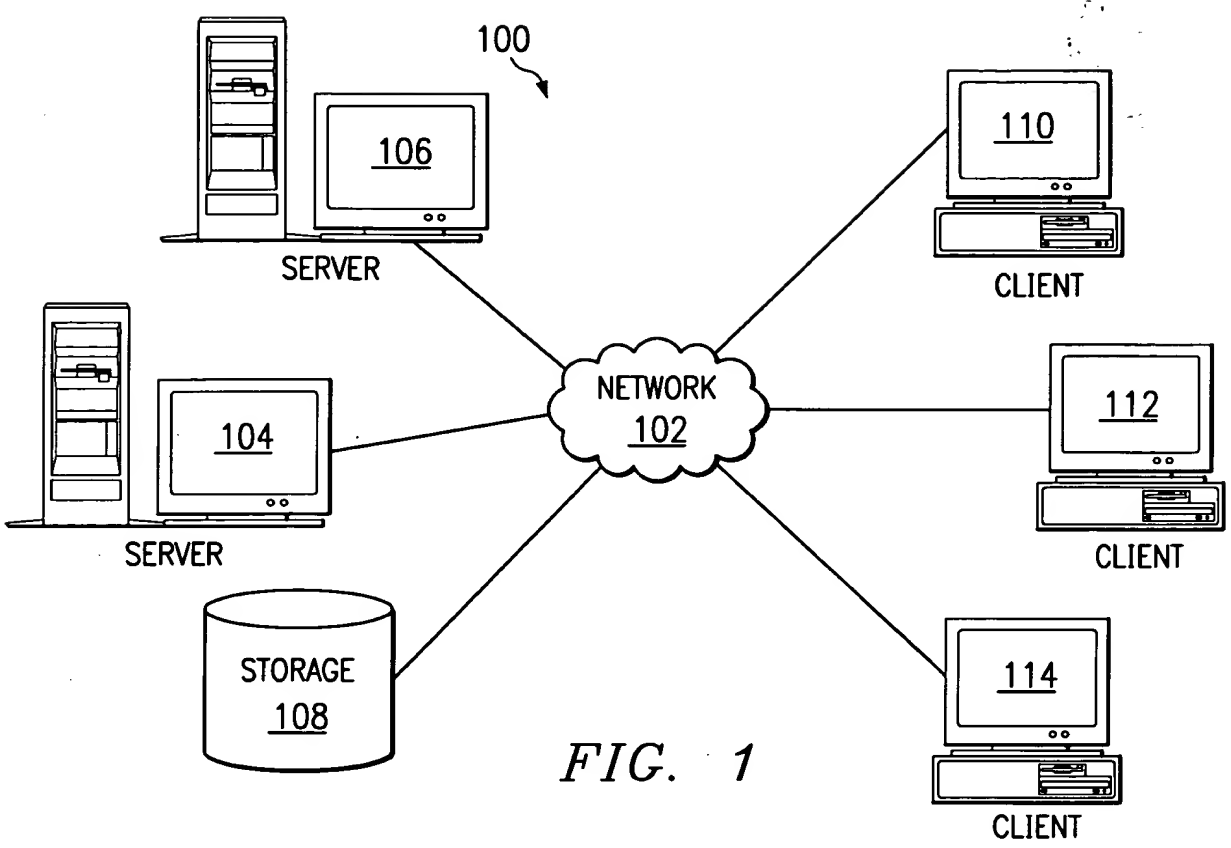

100
106
SERVER
110
CLIENT
NETWORK
102
104
SERVER
112
CLIENT
STORAGE
108
114
CLIENT

FIG. 1

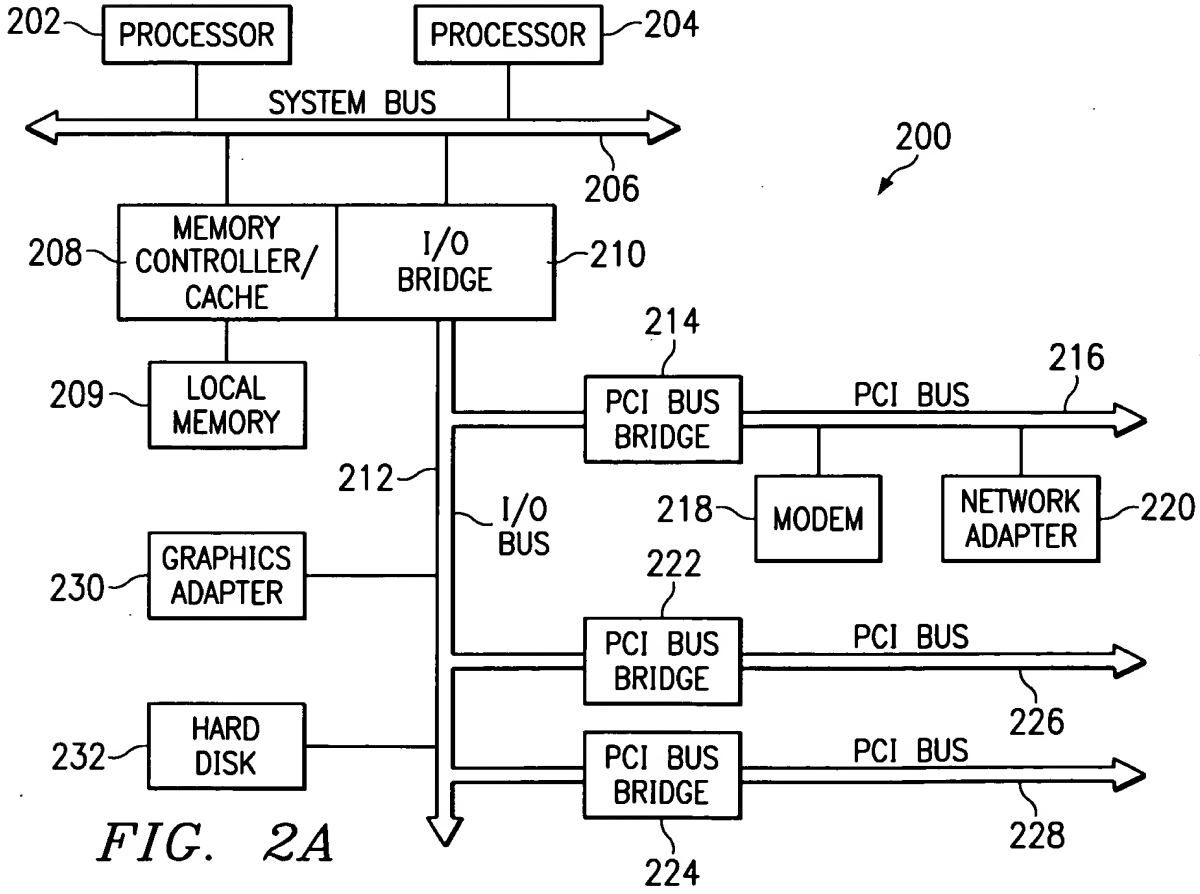

202
PROCESSOR
PROCESSOR
204
SYSTEM BUS
206
200
208
MEMORY CONTROLLER/ CACHE
I/O BRIDGE
210
214
209
LOCAL MEMORY
PCI BUS BRIDGE
PCI BUS
216
212
I/O BUS
218
MODEM
NETWORK ADAPTER
220
222
230
GRAPHICS ADAPTER
PCI BUS BRIDGE
PCI BUS
226
232
HARD DISK
PCI BUS BRIDGE
PCI BUS
228
224

FIG. 2A

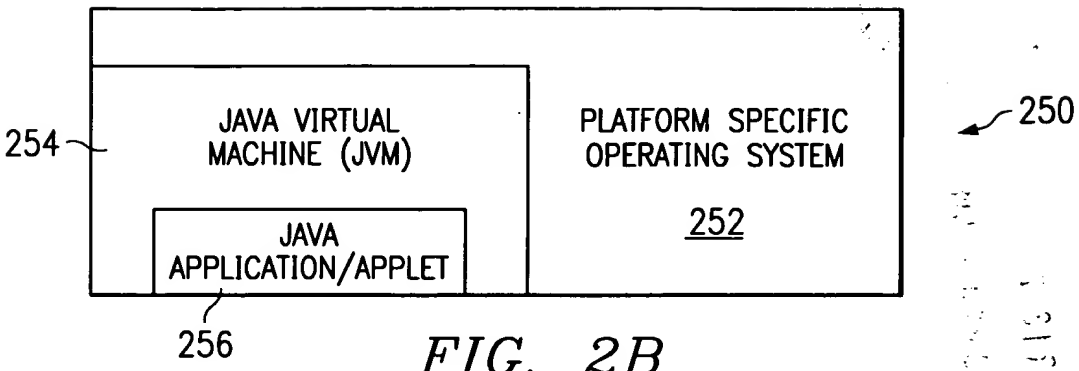


FIG. 2B

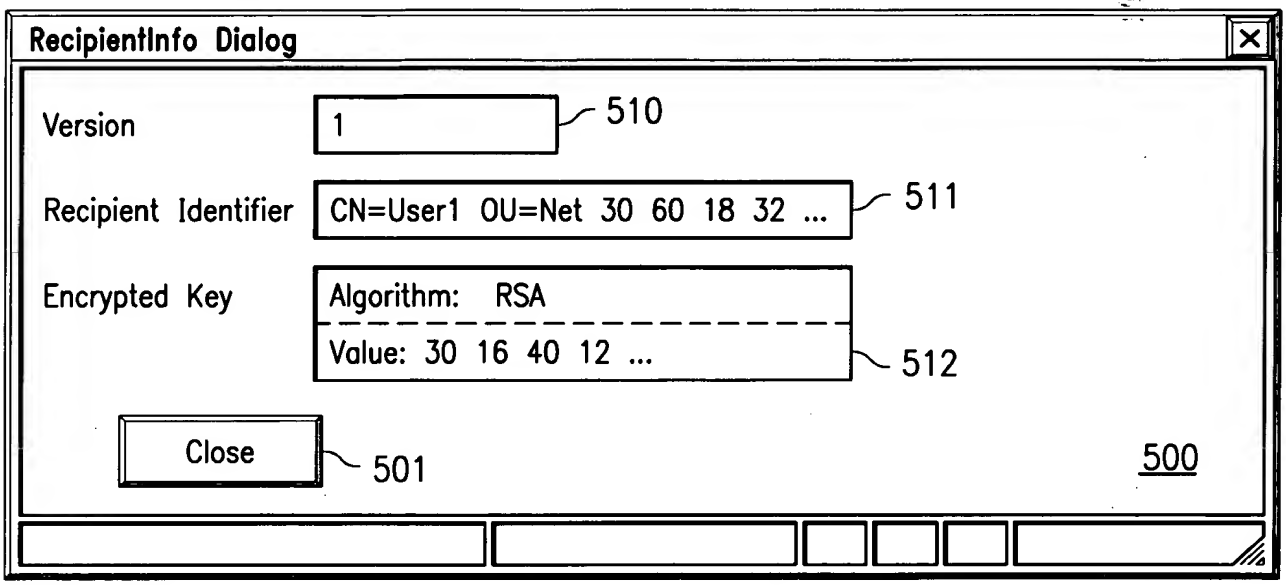


FIG. 5A

```
RecipientInfo ::= CHOICE {
    ktri KeyTransRecipientInfo,
    kari [1] KeyAgreeRecipientInfo,
    kekri [2] KEKRecipientInfo }

KeyTransRecipientInfo ::= SEQUENCE {
    version CMSVersion, -- always set to 0 or 2
    rid RecipientIdentifier,
    keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
    encryptedKey EncryptedKey }

RecipientIdentifier ::= CHOICE {
    issuerAndSerialNumber IssuerAndSerialNumber,
    subjectKeyIdentifier [0] SubjectKeyIdentifier }
```

FIG. 5B

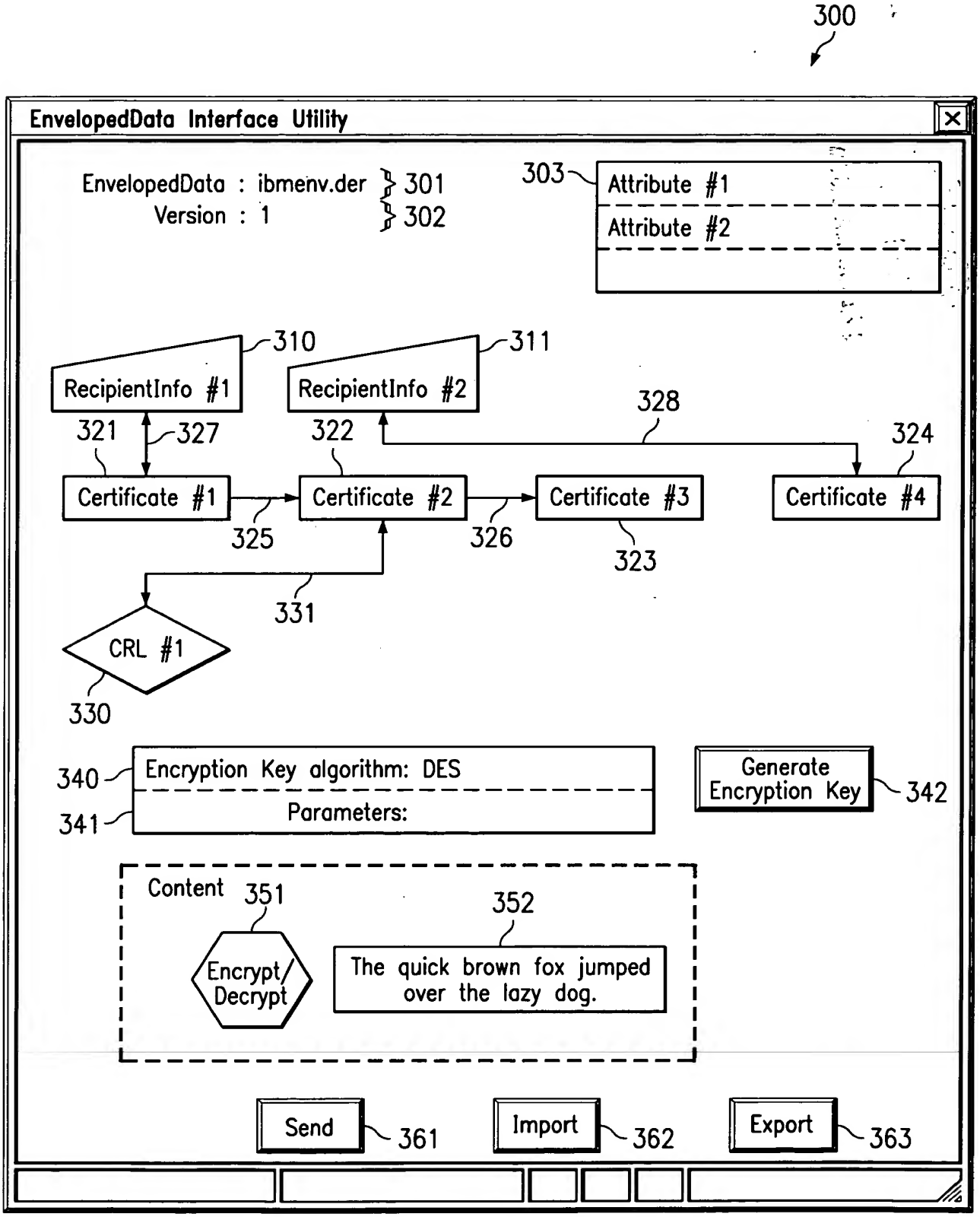

300
EnvelopedData Interface Utility
EnvelopedData : ibmenv.der
Version : 1
301
302
303
Attribute #1
Attribute #2
310
311
RecipientInfo #1
RecipientInfo #2
328
321
327
322
324
Certificate #1
Certificate #2
Certificate #3
Certificate #4
325
326
323
331
CRL #1
330
340
Encryption Key algorithm: DES
341
Parameters:
Generate Encryption Key
342
Content
351
352
Encrypt/ Decrypt
The quick brown fox jumped over the lazy dog.
Send
361
Import
362
Export
363

FIG. 3

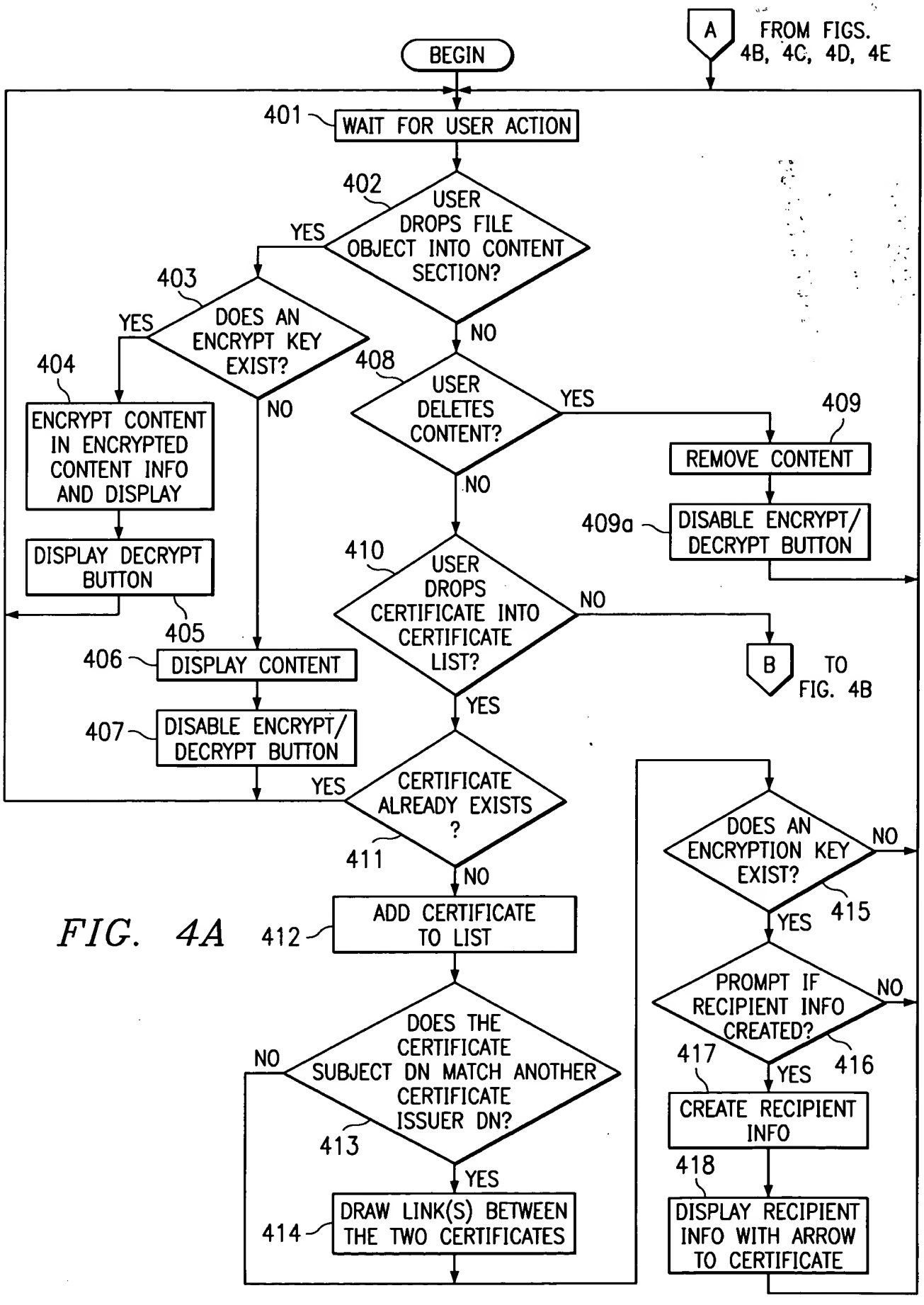

A
FROM FIGS. 4B, 4C, 4D, 4E
BEGIN
401
WAIT FOR USER ACTION
402
USER DROPS FILE OBJECT INTO CONTENT SECTION?
YES
NO
403
DOES AN ENCRYPT KEY EXIST?
YES
NO
404
ENCRYPT CONTENT IN ENCRYPTED CONTENT INFO AND DISPLAY
DISPLAY DECRYPT BUTTON
405
406
DISPLAY CONTENT
407
DISABLE ENCRYPT/ DECRYPT BUTTON
408
USER DELETES CONTENT?
YES
NO
409
REMOVE CONTENT
409a
DISABLE ENCRYPT/ DECRYPT BUTTON
410
USER DROPS CERTIFICATE INTO CERTIFICATE LIST?
NO
B
TO FIG. 4B
YES
CERTIFICATE ALREADY EXISTS ?
YES
411
NO
412
ADD CERTIFICATE TO LIST
DOES THE CERTIFICATE SUBJECT DN MATCH ANOTHER CERTIFICATE ISSUER DN?
NO
413
YES
414
DRAW LINK(S) BETWEEN THE TWO CERTIFICATES
DOES AN ENCRYPTION KEY EXIST?
NO
415
YES
PROMPT IF RECIPIENT INFO CREATED?
NO
416
417
YES
CREATE RECIPIENT INFO
418
DISPLAY RECIPIENT INFO WITH ARROW TO CERTIFICATE

FIG. 4A

FIG. 4B

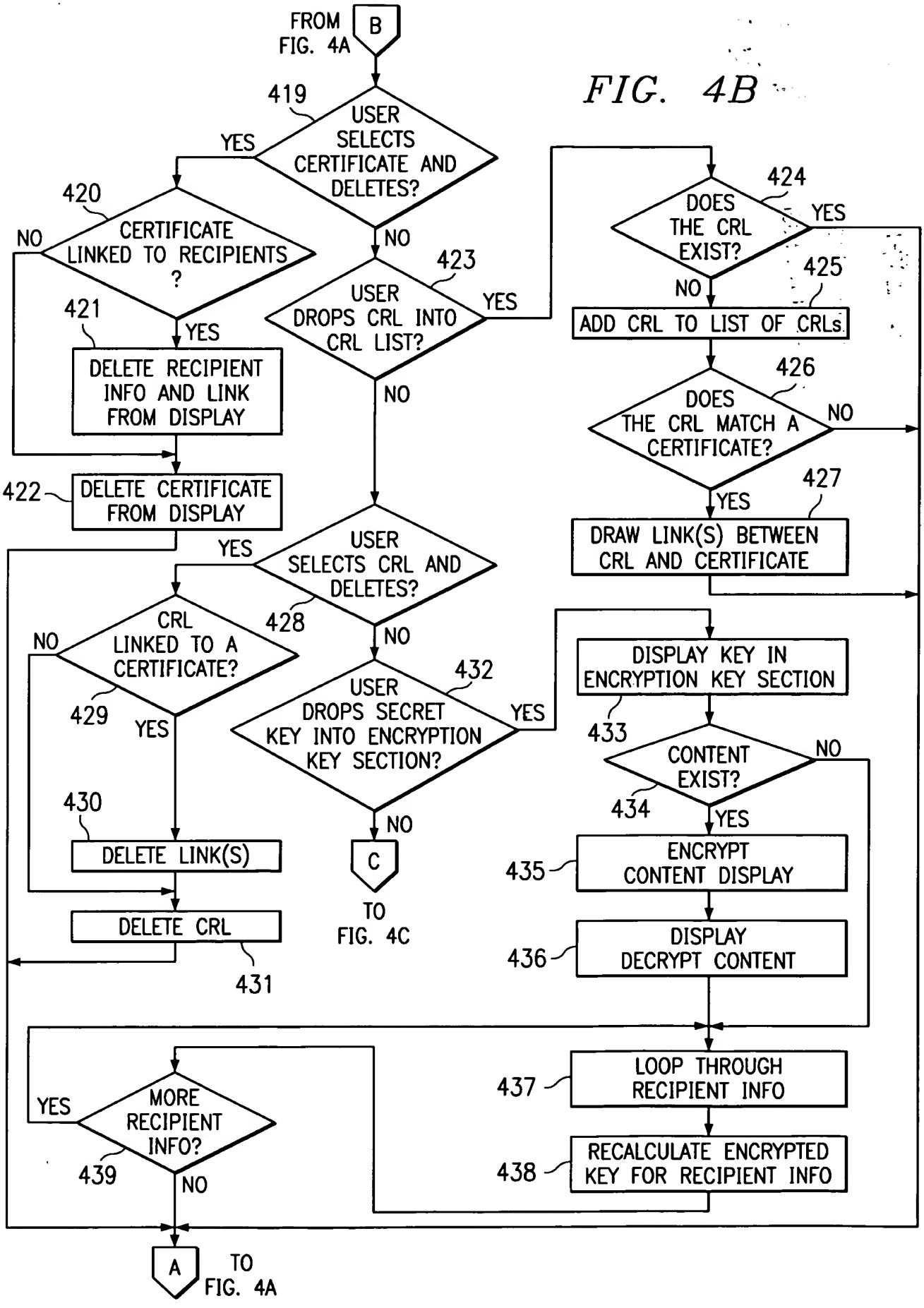
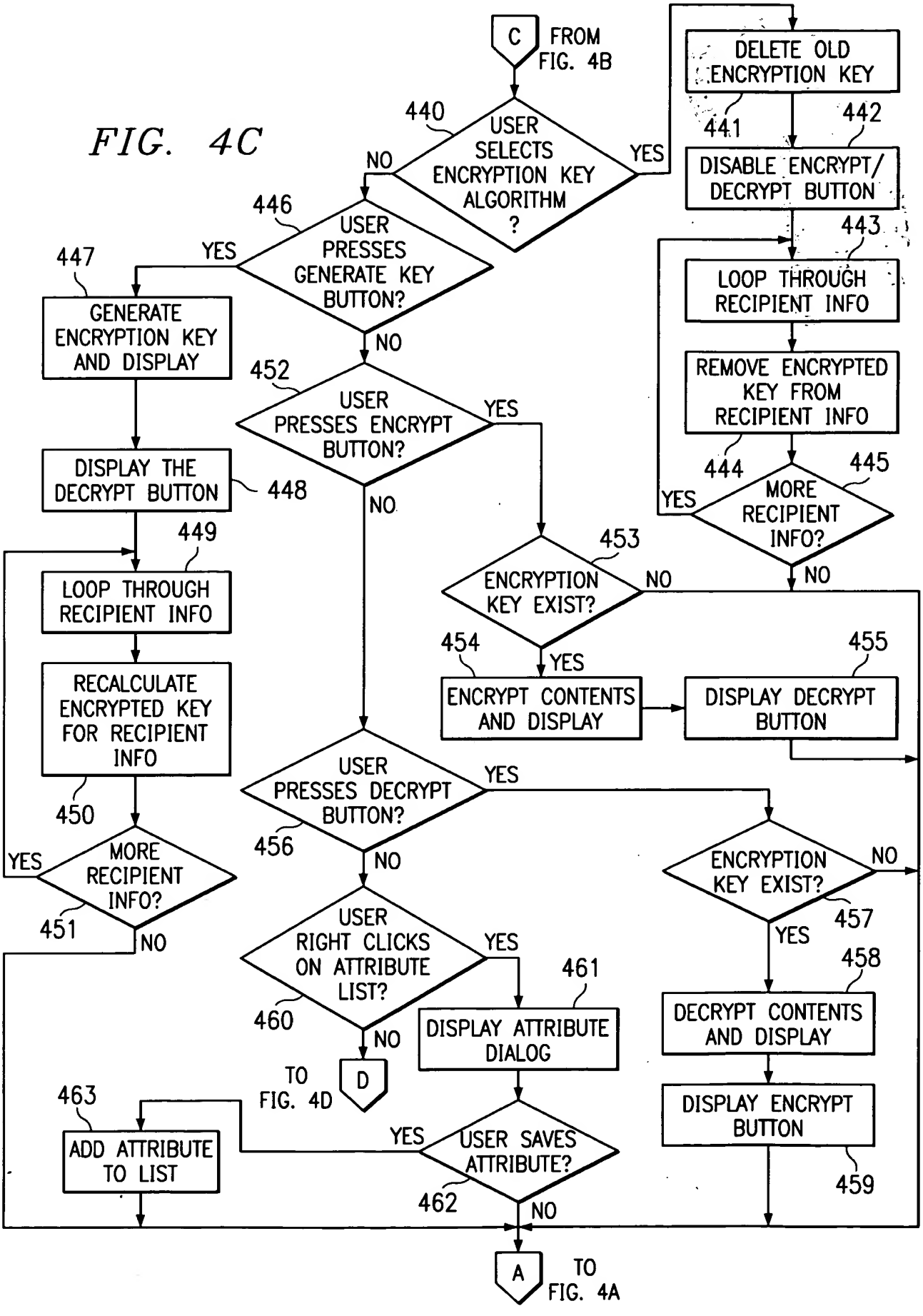

FROM FIG. 4A
B
419
USER SELECTS CERTIFICATE AND DELETES?
YES
NO
420
CERTIFICATE LINKED TO RECIPIENTS ?
NO
YES
421
DELETE RECIPIENT INFO AND LINK FROM DISPLAY
422
DELETE CERTIFICATE FROM DISPLAY
423
USER DROPS CRL INTO CRL LIST?
YES
NO
424
DOES THE CRL EXIST?
YES
NO
425
ADD CRL TO LIST OF CRLs
426
DOES THE CRL MATCH A CERTIFICATE?
NO
YES
427
DRAW LINK(S) BETWEEN CRL AND CERTIFICATE
USER SELECTS CRL AND DELETES?
YES
NO
428
CRL LINKED TO A CERTIFICATE?
NO
YES
429
430
DELETE LINK(S)
DELETE CRL
431
USER DROPS SECRET KEY INTO ENCRYPTION KEY SECTION?
YES
NO
432
C
TO FIG. 4C
DISPLAY KEY IN ENCRYPTION KEY SECTION
433
CONTENT EXIST?
NO
YES
434
435
ENCRYPT CONTENT DISPLAY
436
DISPLAY DECRYPT CONTENT
437
LOOP THROUGH RECIPIENT INFO
438
RECALCULATE ENCRYPTED KEY FOR RECIPIENT INFO
MORE RECIPIENT INFO?
YES
NO
439
A
TO FIG. 4A

FIG. 4C


C
FROM FIG. 4B
440
USER SELECTS ENCRYPTION KEY ALGORITHM ?
YES
NO
DELETE OLD ENCRYPTION KEY
441
442
DISABLE ENCRYPT/ DECRYPT BUTTON
443
LOOP THROUGH RECIPIENT INFO
REMOVE ENCRYPTED KEY FROM RECIPIENT INFO
444
445
MORE RECIPIENT INFO?
YES
NO
446
USER PRESSES GENERATE KEY BUTTON?
YES
NO
447
GENERATE ENCRYPTION KEY AND DISPLAY
452
USER PRESSES ENCRYPT BUTTON?
YES
NO
DISPLAY THE DECRYPT BUTTON
448
449
LOOP THROUGH RECIPIENT INFO
RECALCULATE ENCRYPTED KEY FOR RECIPIENT INFO
450
MORE RECIPIENT INFO?
YES
NO
451
453
ENCRYPTION KEY EXIST?
NO
YES
454
ENCRYPT CONTENTS AND DISPLAY
455
DISPLAY DECRYPT BUTTON
USER PRESSES DECRYPT BUTTON?
YES
NO
456
ENCRYPTION KEY EXIST?
NO
YES
457
458
DECRYPT CONTENTS AND DISPLAY
DISPLAY ENCRYPT BUTTON
459
USER RIGHT CLICKS ON ATTRIBUTE LIST?
YES
NO
460
461
DISPLAY ATTRIBUTE DIALOG
TO FIG. 4D
D
463
ADD ATTRIBUTE TO LIST
USER SAVES ATTRIBUTE?
YES
NO
462
A
TO FIG. 4A

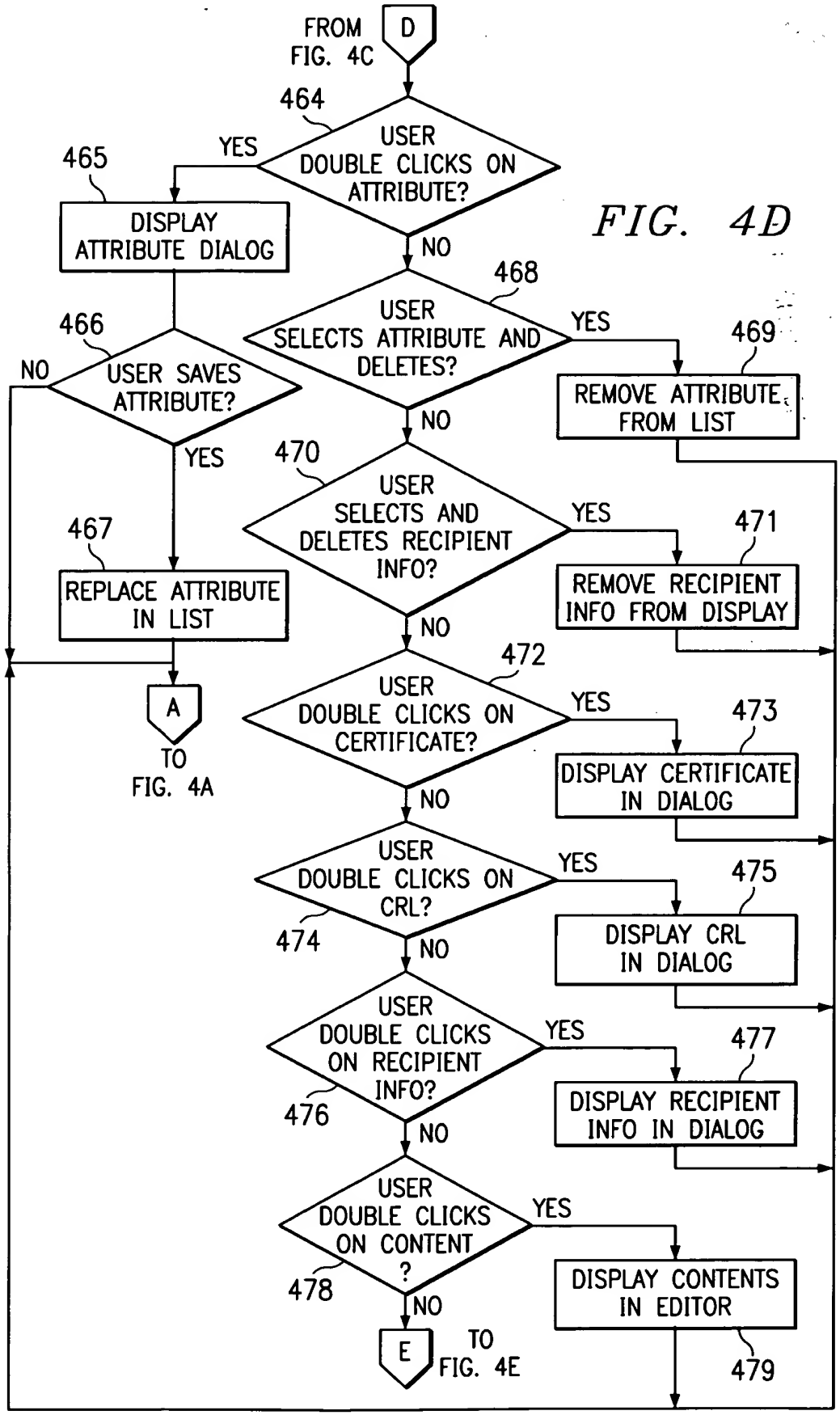

FROM FIG. 4C
D
464
USER DOUBLE CLICKS ON ATTRIBUTE?
YES
465
DISPLAY ATTRIBUTE DIALOG
NO
468
USER SELECTS ATTRIBUTE AND DELETES?
YES
469
REMOVE ATTRIBUTE FROM LIST
466
USER SAVES ATTRIBUTE?
NO
YES
470
USER SELECTS AND DELETES RECIPIENT INFO?
YES
471
REMOVE RECIPIENT INFO FROM DISPLAY
467
REPLACE ATTRIBUTE IN LIST
NO
472
USER DOUBLE CLICKS ON CERTIFICATE?
YES
473
DISPLAY CERTIFICATE IN DIALOG
A
TO FIG. 4A
NO
USER DOUBLE CLICKS ON CRL?
YES
475
DISPLAY CRL IN DIALOG
474
NO
USER DOUBLE CLICKS ON RECIPIENT INFO?
YES
477
DISPLAY RECIPIENT INFO IN DIALOG
476
NO
USER DOUBLE CLICKS ON CONTENT ?
YES
DISPLAY CONTENTS IN EDITOR
478
NO
E
TO FIG. 4E
479

FIG. 4D

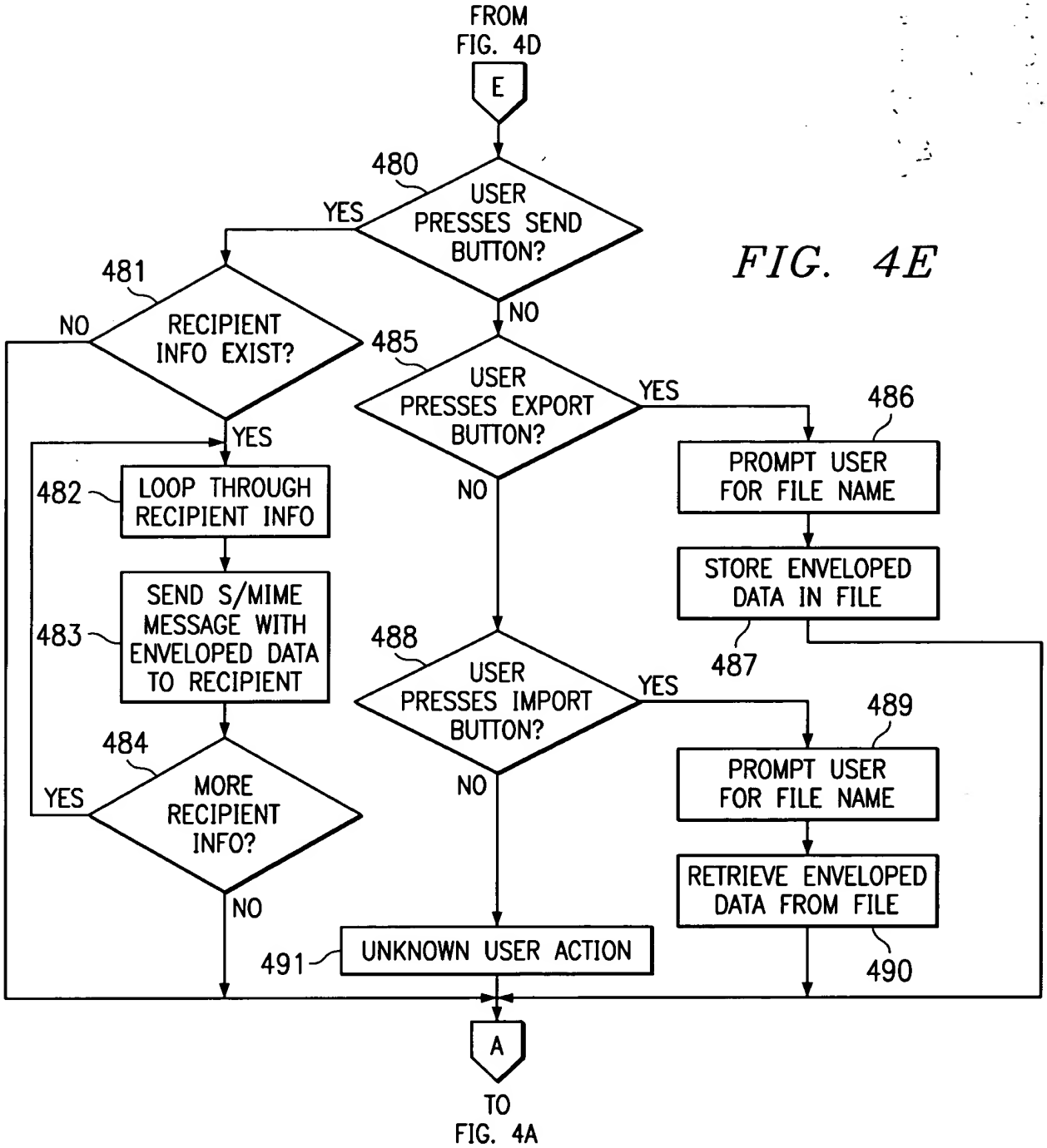

FROM
FIG. 4D
E
480
USER
PRESSES SEND
BUTTON?
YES
NO
481
RECIPIENT
INFO EXIST?
NO
YES
482
LOOP THROUGH
RECIPIENT INFO
483
SEND S/MIME
MESSAGE WITH
ENVELOPED DATA
TO RECIPIENT
484
MORE
RECIPIENT
INFO?
YES
NO
485
USER
PRESSES EXPORT
BUTTON?
YES
NO
486
PROMPT USER
FOR FILE NAME
STORE ENVELOPED
DATA IN FILE
487
488
USER
PRESSES IMPORT
BUTTON?
YES
NO
489
PROMPT USER
FOR FILE NAME
RETRIEVE ENVELOPED
DATA FROM FILE
490
491
UNKNOWN USER ACTION
A
TO
FIG. 4A

FIG. 4E

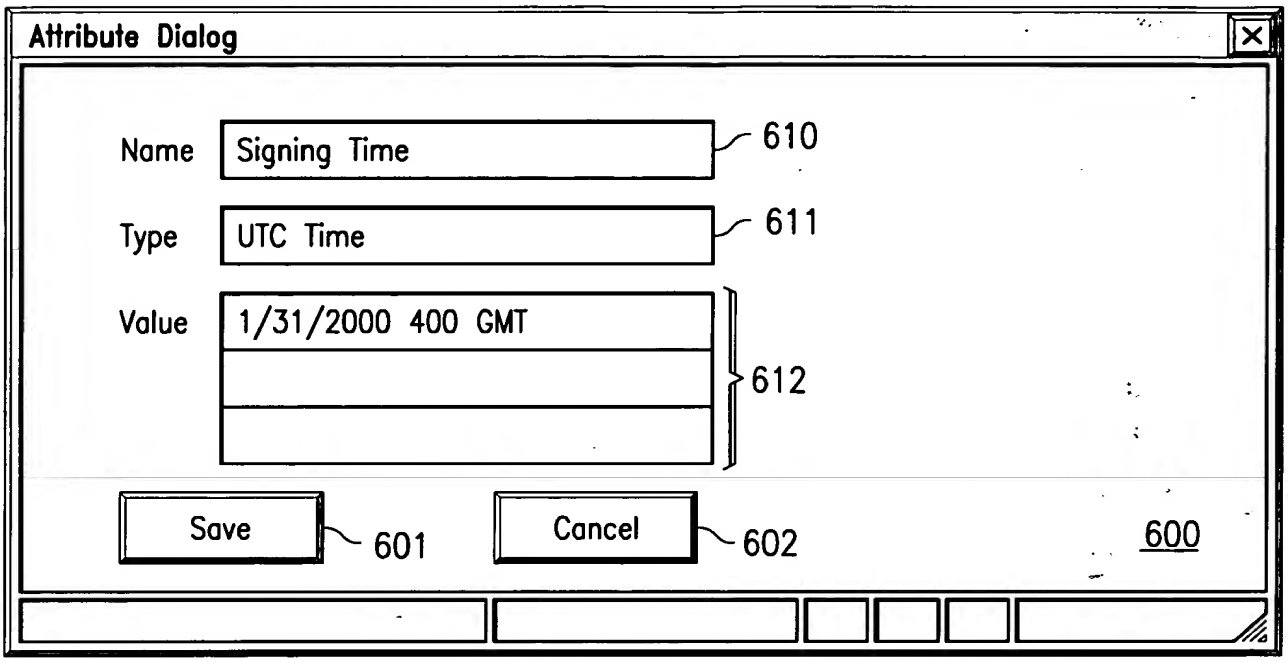

Attribute Dialog
Name
Signing Time
610
Type
UTC Time
611
Value
1/31/2000 400 GMT
612
Save
601
Cancel
602
600

FIG. 6

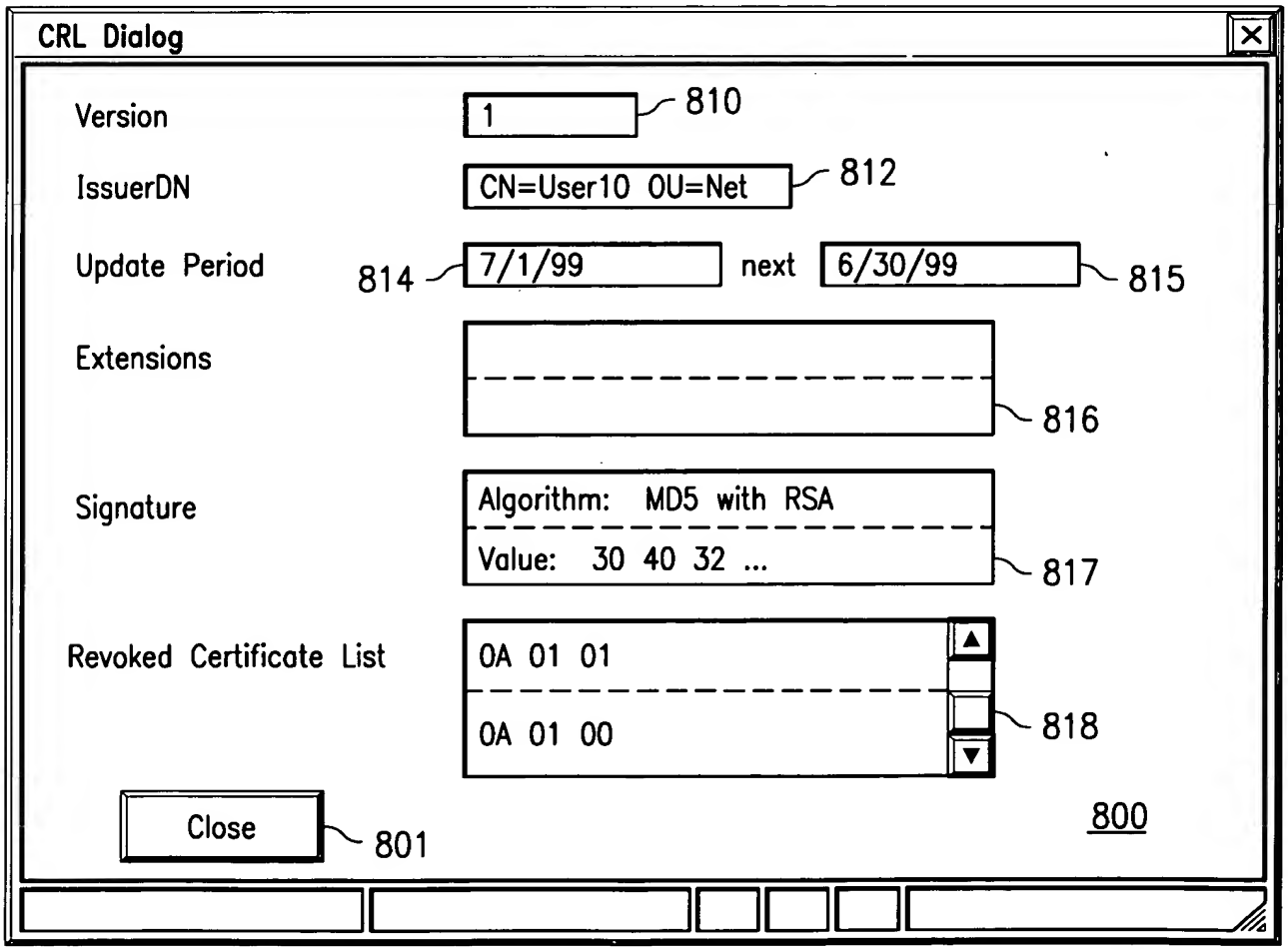

CRL Dialog
Version
1
810
IssuerDN
CN=User10 OU=Net
812
Update Period
814
7/1/99
next
6/30/99
815
Extensions
816
Signature
Algorithm: MD5 with RSA
Value: 30 40 32 ...
817
Revoked Certificate List
0A 01 01
0A 01 00
818
Close
801
800

FIG. 8

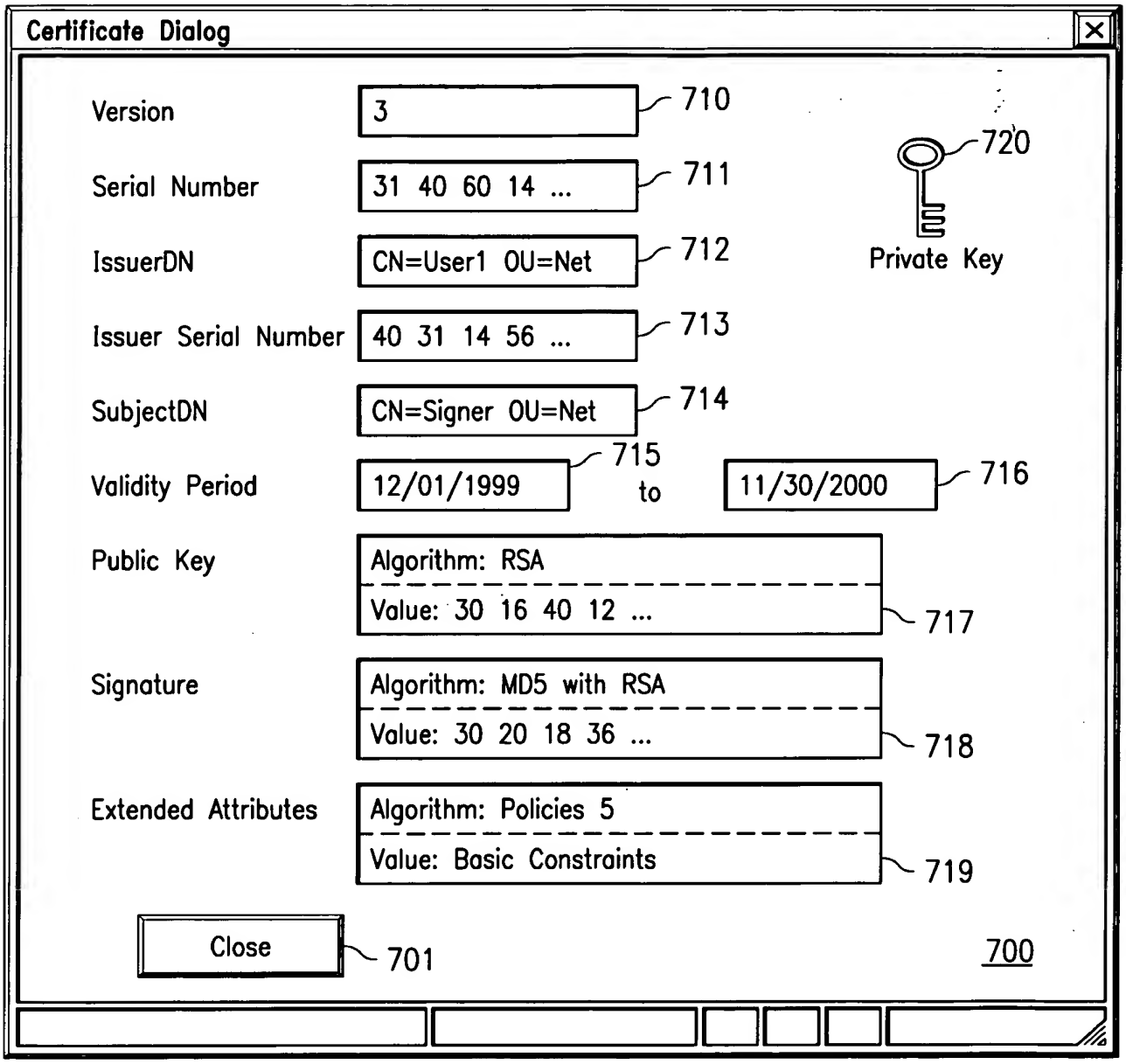

Certificate Dialog
Version
3
710
Serial Number
31 40 60 14 ...
711
IssuerDN
CN=User1 OU=Net
712
Issuer Serial Number
40 31 14 56 ...
713
SubjectDN
CN=Signer OU=Net
714
Validity Period
12/01/1999
715
to
11/30/2000
716
Public Key
Algorithm: RSA
Value: 30 16 40 12 ...
717
Signature
Algorithm: MD5 with RSA
Value: 30 20 18 36 ...
718
Extended Attributes
Algorithm: Policies 5
Value: Basic Constraints
719
720
Private Key
Close
701
700

FIG. 7